War-Winning Capabilities … On Time, On Cost

Accreditation of Instrumentation Systems and a Few Ways Vendors Can Help

15 May 2019

Todd Jacob
812 AITS/ENIE

U.S. AIR FORCE

Overview

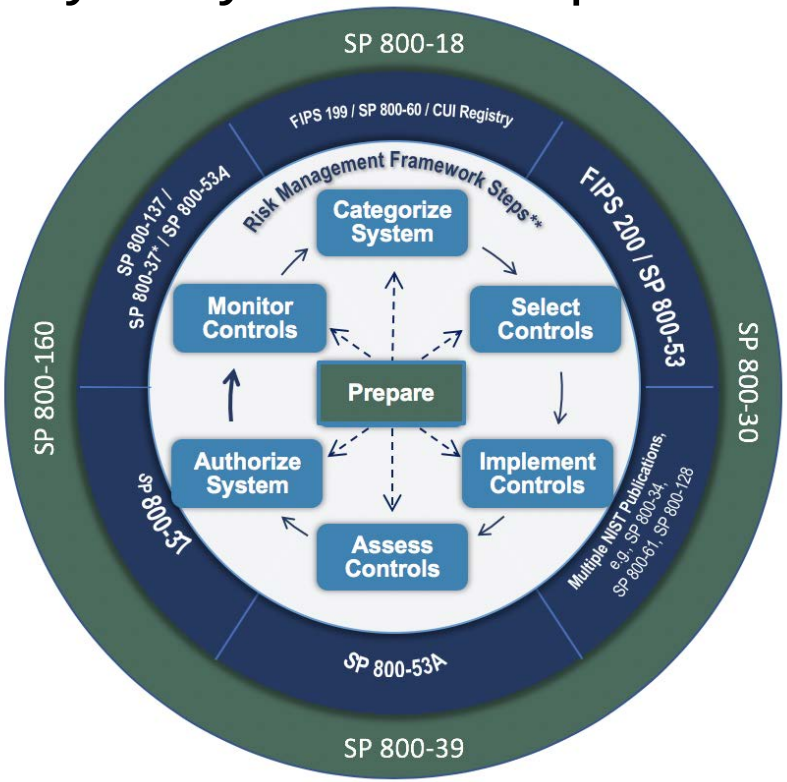
- RMF Accreditation Process
- RMF and Vendors
- Common Software Accreditation Issues
  - Increasing Risk
  - Unsupported Components
  - Vulnerable Components
  - Managing Components
  - Installation issues
  - Software Delivery
- Event Logging
- Non-Volatile Memory (NVM)
  - Characterize NVM
  - Isolating NVM
- Takeaways

RMF Accreditation Process

- **RMF and Authority To Operate (ATO) Accreditation**

  The DoD uses the NIST Risk Management Framework (RMF) to improve cybersecurity of systems. Steps include:

  – Prepare
  – Categorization
  – Select Controls
  – Implementation
  – Assess
  – Authorization (ATO)
  – Monitoring



https://csrc.nist.gov/Projects/Risk-Management/rmf-quick-start-guides

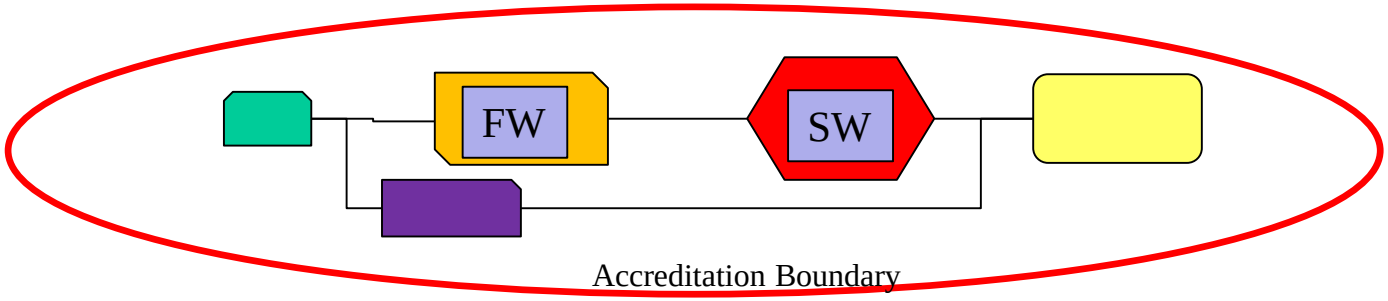
RMF Accreditation Process

- **Controls in RMF**
  - **Aprx 1500 controls and enhancements categorized into 18 families**
  - **The design and configuration options of vendors products can help the DoD meet a sub-set of RMF controls**
  - **V5 out soon**

https://nvd.nist.gov/800-53/Rev4

RMF Accreditation Process

- **The DoD Accredits Systems**
  - **Systems are made up of components and software**
  - **Systems are accredited, individual components are not accredited**
  - **The Approving Official (AO) is a senior member of the DoD**
  - **When making a accreditation decision, AO consider the cybersecurity of the components-software-processes, the sensitivity of the system, and the threat environment**



RMF and Vendors

- **Talk with your customers to understand which controls they need vendor help to implement**
  - **Cost vs. benefit tradeoff**
- **Provide options so customers can:**
  - **Install only required components to reduce attack surface and the number of controls that need to be addressed**
  - **Configure features that implement controls such as event logging, enhanced authentication methods…**

Order Form

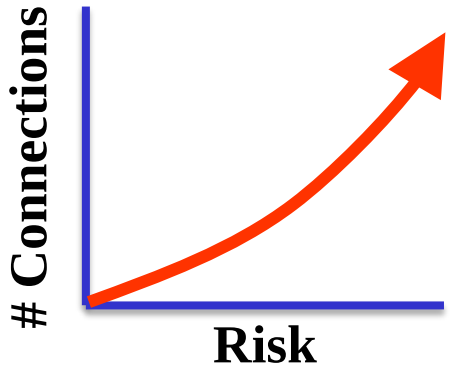
Replaceable Firmware Module
Manual Firmware Update Switch

Installation Options

- [ ] Command Line Interface
- [x] Web Interface
- [x] Standalone database
- [ ] Network Database
- [2] Event Logging Level

Software – Increasing Risk

- **Increase in network connectivity is increasing risk**



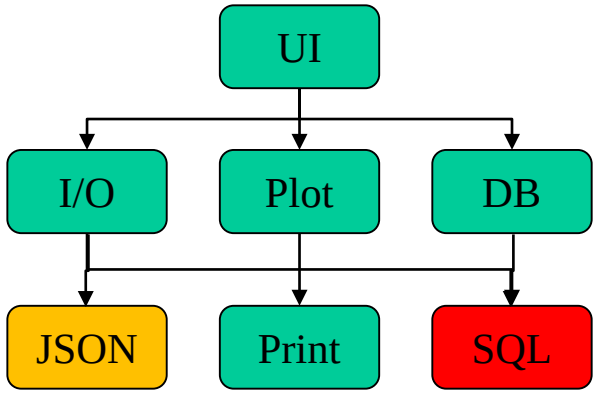
- **RMF addresses software vulnerabilities**
  - **SI-2 Flaw Remediation**
  - **SA-22 Unsupported System Components**
- **The following accreditation issues are derived from system accreditation efforts, Risk Mitigation Boards (RMB), and software approval activities**

Software - Unsupported Components

- **Unsupported Software Components, Common Findings**
  - **Outdated Microsoft Visual C++ Redistributables**
  - **Outdated Java JRE or JDK (Java SE version)**
  - **Outdated ActiveX Components**
  - **Outdated Adobe Reader, Acrobat, Flash**
  - **Outdated OpenSSL**
    - **0.9.8, 1.0.0 and 1.0.1 versions are now out of support**
    - **1.0.2 series out of support on 31st December 2019**
    - **1.1.0 series out of support on 11th September 2019**
  - **Outdated Apache Webserver**
  - **Outdated SSH Components**
  - **…**

Software - Vulnerable Components

- **Vulnerable 3rd Party SW Components, Common Findings**
  - **Microsoft 2010 Visual C++ Redistributables**
    - **CVE-2010-3190, CVE-2010-3190, (upgrade to latest version)**
  - **Microsoft ActiveX Components**
    - **mscomct2.ocx, CVE-2008-4255,**
    - **richtx32.ocx, CVE-2008-0237**
  - **Adobe Products**
    - **Too many CVE to list**
  - **Java**
    - **Too many CVE to list**
  - **…**



Software – Managing Components

- Supporting 3rd Party Components
  - AO generally want “adequate maintenance & support”
  - No agreed upon definition of this requirement
  - When asked, describe how you support 3rd party components
- Good Practices
  - Have a complete inventory of 3rd party software
  - Monitor for bugs and updates
  - Incorporate security patches soon after publication
  - Upgrade/replace/remove components that are no longer supported
  - Try to use system-managed components, or allow system administrators to update components

Software – Installation Issues

- **Non-standard firewall rules**
  - **Firewall rule with “Any” is an issue for some AO**
  - **Use standard ports, protocols and services**
    - **DoDI 8551.01 (https://iase.disa.mil/ppsm, sections may require a CAC login)**
- **Software Installation Locations**
  - **Software should install in the proper C:\Program Files for Windows**
  - **Follow the Linux file system hierarchy standard**
- **Do not write data to non-standard locations**
  - **Writing to the root of C:\ is not accepted**
  - **Self Modifying Code is a security risk**

Software – Installation Issues

- **Running software as Admin is not advised**
  - **Software must be executable as regular user**
  - **Security+ certifications may be required for admin**
- **Windows Operating Systems Not Named “10”**
  - **Windows 8 is unsupported**
  - **Windows 7 support ends Jan 4th 2020**
  - **Windows 10 1607 unsupported, 1703 Oct 2019**
- **Hard coded passwords are not allowed**

Software – Delivery

- RMF addresses the secure delivery of firmware and software (SI-7)
- Secure methods for delivering firmware/software
  - Secure software update process
    - See https://cwe.mitre.org/data/definitions/494.html
  - Checksum delivered via separate channel
    - Don't transmit the checksum using the same system used to host the software
    - Win10 use *CertUtil –hashfile Infile [HashAlgorithm]*
  - Physical delivery
- Firmware to be installed/updated over a network
  - Consider an option that requires a physical presence for updating firmware: switch, jumper, separate port…

Event Logging

- **RMF Addresses Continuous Monitoring**
  - **Audit and Accountability control family**
    - **AU-1 thru AU-16**
- **Allow customers to configure event logging**
  - **Log device specific events**
    - **recording on/off, camera resolution changes…**
  - **Log configuration changes**
  - **Log firmware or software upgrades**
  - **Log device usage**
    - **admin logins, starts, stops…**

Non-Volatile Memory (NVM)

- **NVM Cybersecurity Issues**
  - **NVM is a potential pathway for information to be transported between security boundaries**
  - **A greater use of third party parts and software has increased risk**
  - **Consider ramifications to NVM if firmware is pw0ned**
- **Characterize NVM**
  - **Look deeper into designs to identify all NVM, provide detailed descriptions in the Letter of Volatility**
  - **Understand and document how NVM can be written-to, or read-from, via software, identify pathways**
  - **There will be a greater emphasis on providing documentation that supports Letters of Volatility**

Non-Volatile Memory (NVM)

412TW

- **Provide tools to examine and/or validate NVM**
  - **Some customers may require the ability to examine the contents of NVM or use checksums to validate the contents of NVM**
  - **Used when sending and receiving equipment**
- **Encryption**
  - **Encrypting NVM data and zeroing the key may be an option**
  - **Acceptance of this method is system and AO dependent**
  - **Talk with your customers**
- **Allow for Customer Applied Firmware Updates**
  - **Sending equipment with NVM back to the manufacture for firmware updates constraints customers**
  - **Consider methods to allow firmware updates to easily take place at customer locations**

Non-Volatile Memory (NVM)

- **Localize NVM in Removable Packaging**
  - **To ease physical protection requirements, the ability to move equipment between security boundaries, and the ability to send equipment back for repair, consider localizing NVM in removable packaging**
  - **Data recorder Removable Media Modules (RMM) is a good example for bulk data**
  - **For internal NVM such as firmware loads, configuration data, and maintenance logs, consider USB flash devices, SD cards, daughter cards, or removable chips**
  - **Consider designs that allow removing NVM without extracting the device from the SUT**
  - **As always, talk to your customers**

Takeaways

- The configuration of products can help or hinder the accreditation of instrumentation systems
  - Talk with customers
  - Provide options that assist RMF accreditation
- Software
  - Manage software components
  - Chose secure software installation practices
  - Provide secure delivery of firmware and software
- Characterize NVM, Removable NVM, NVM Tools
- Resources and Ideas
  - Secure coding class for developers
  - CWE https://cwe.mitre.org/index.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09/05/2019	Slides	15 May 2019

4. TITLE AND SUBTITLE
Accreditation of Instrumentation Systems and a Few Ways Vendors Can Help

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Todd Jacob

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
812th AITS
300 E Yeager Ave
Edwards AFB CA 93524

8. PERFORMING ORGANIZATION REPORT NUMBER
412TW-PA-19260

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
812th AITS
300 E Yeager Ave
Edwards AFB CA 93524

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release A: distribution is unlimited.

13. SUPPLEMENTARY NOTES
ITEA, 14-16 May 2019. Las Vegas NV

14. ABSTRACT
The USAF requires a cybersecurity Risk Management Framework (RMF) accreditation package to be approved by Authorizing Official (AO) to grant an Authority to Operate (ATO) for all instrumentation systems installed on USAF platforms. Vendors can help the USAF obtain an ATO by delivering software and hardware that implements best cybersecurity practices such as delivering software with reduced attack surface, secure delivery of software binaries, and secure methods for installing/validating firmware. Hardware designs can assist the accreditation processes by defining non-volatile memory (NVM) characteristics and reduce the operational issues by isolating NVM. Adding options for logging control-plane and data-plane network traffic is very helpful as instrumentation systems expand the use of connected networks.

15. SUBJECT TERMS
Authority to Operate (ATO), Non-Volatile Memory (NVM)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					412 TENG/EN (Tech Pubs)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	None	19	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			661-277-8615